

Integrating Trend Micro™ Email Security with Google™ G Suite

This guide provides the steps necessary to configure Google™ G Suite to work with Trend Micro™ Email Security.



Copyright ©2020 by Trend Micro Incorporated. All rights reserved.

Trend Micro, the Trend Micro t-ball logo, Trend Micro Security, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Information in this document is subject to change without notice.

Table of Contents

| | |
|--|----|
| Introduction to Trend Micro Email Security | 4 |
| How Trend Micro Email Security Works | 4 |
| Redirecting your MX record to Trend Micro Email Security | 5 |
| Commonly Used DNS Providers | 6 |
| Go Daddy | 6 |
| Network Solutions | 7 |
| Enom | 7 |
| DreamHost | 7 |
| Yahoo! Small Business | 8 |
| Configuring Trend Micro Email Security to Forward Inbound E-mails to Google Apps Mail Servers | 8 |
| Configuring Google Apps Mail Servers to Accept Inbound E-mails from Trend Micro Email Security | 9 |
| Testing the Message Route | 11 |
| Scanning Outbound E-mail from Google Apps Mail Servers | 12 |
| Configure your Trend Micro Email Security Settings | 12 |
| Configure Google Apps Settings | 12 |

Introduction to Trend Micro Email Security

E-mail is mission critical, but the volume of spam and e-mail-based malware is growing. At the same time, other critical projects and tasks consume time in the administration of a network. However, e-mail security maintenance should not be neglected. Doing so will lead to a decline in your e-mail protection and spam-blocking effectiveness.

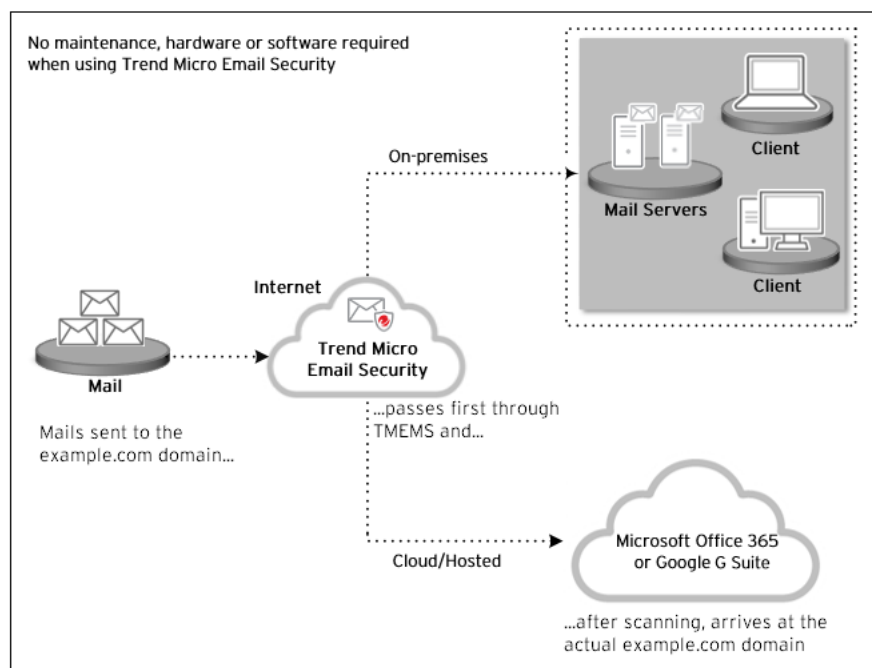
Trend Micro Email Security is a no-maintenance-required solution that delivers continuously updated protection to stop spam, malware, spear-phishing and advanced targeted attacks before they reach your network. It protects Microsoft Exchange, Microsoft Office 365, Google G Suite and other hosted and on-premises e-mail solutions.

Unlike traditional self-hosted e-mail solutions where a simple cable could be moved in order to add a layer of protection, cloud-based solutions require a different approach.

This guide highlights step-by-step instructions on integration of Trend Micro Email Security with Google G Suite. It assumes a functioning G Suite deployment.

How Trend Micro Email Security Works

The figure below shows the flow of messaging traffic from the Internet, through the Trend Micro Email Security Servers and then to the Google Apps Mail Servers.



The processes performed by Trend Micro Email Security are explained below:

1. The originating mail server performs a DNS lookup to determine the location of the *example.com* domain. Since Trend Micro Email Security must intercept your company's e-mails before delivery, the Mail



Exchange (MX) record for *example.com* holds the IP address of Trend Micro Email Security instead of the original IP address for *example.com*.

2. The originating mail server routes the e-mails to Trend Micro Email Security.
3. Trend Micro Email Security Servers accept the message and perform message filtering and policy matching on your behalf.
4. Assuming a message is slated for delivery according to its security policy or validity status, the Trend Micro Email Security Servers route the message to the Google Apps Mail Servers.

Redirecting your MX record to Trend Micro Email Security

In order for Trend Micro Email Security to scan e-mails bound for your domain, you must update your MX record to deliver e-mails to the Trend Micro Email Security Servers.

Here are the steps on how to redirect your MX record:

1. Check your Trend Micro Email Security welcome e-mail which contains the specific MX record information. You also refer to the following MX records based on the region:
 - North America, Latin America and Asia Pacific:
<company_identifier>.in.tmes.trendmicro.com
 - Europe, the Middle East and Africa:
<company_identifier>.in.tmes.trendmicro.eu
 - Australia and New Zealand:
<company_identifier>.in.tmes-anz.trendmicro.com
2. Update your MX record through one of the following ways:
 - a. **Through a Support Technician:** If you are unsure how to configure the MX records for your domain, contact your Internet Service Provider's (ISP) helpdesk or your Domain Name System (DNS) technician for assistance. If your DNS is managed by a third-party or ISP, either they can do this for you or they may have a simple web interface allowing you to make the change yourself. It can take up to 48 hours for any changes to propagate throughout the system.
 - b. **Manual Configuration:** If you manage your own DNS, you can manually edit your MX record (this applies to self-managed, smaller accounts).
3. After making the modifications to the MX record, Trend Micro Email Security becomes the point of entry of e-mails for your domain. After the DNS record modifications take effect (up to 48 hours), all inbound e-mail traffic is routed to Trend Micro Email Security.

Commonly Used DNS Providers

Go Daddy

1. Login to your account at www.godaddy.com.
2. Open the **Domains** tab and select **My Domain Names**. You'll be directed to the Manage Domains page.
3. Click the domain that you would like to use.
4. Click the **Total DNS Control and MX Records** in the box entitled Total DNS Control.
5. Clear all existing MX Records by clicking **Delete**.
6. Click **OK** in the confirmation dialogue box.
7. Once you've deleted all existing records, click **Add New MX Record**. The MX (Mail Exchangers) Record Wizard will appear.
8. For each MX Record, enter the following information:

Note: Supply the MX record information following the information from the Trend Micro Email Security welcome e-mail.

- a. **Priority Value:** type the priority value
- b. **Enter a Host Name:** leave the default setting to @
- c. **Select TTL Value:** set the default Time to Live (TTL) value to 1 Week

TIP: This will appear as 604800 seconds within the DNS system. This means that it will require one week for your MX records to propagate. For future updates to your records, we suggest you enter a shorter time span for the TTL, such as 1 day or 1 hour.

- d. **Enter Goes To Address:** type the Trend Micro Email Security address, including the trailing dots at the end of each record.
9. Click **Continue**. After that, click **Add** to confirm each entry. The DNS Manager main page will reappear when you've finished.

Network Solutions

1. Login to your account at www.networksolutions.com.
2. Click **Edit DNS** under DNS Settings. The Edit DNS page will appear. If you have not previously edited DNS entries for your domain name, you may need to select Custom DNS Setting.
3. Under the **DNS Manager-Advanced Tools** panel, click **Continue**. The DNS Manager-Advanced Tools page will appear.
4. Under the **Mail Servers** panel, click **Add/Edit**. The Mail Servers table will appear.
5. Remove any existing MX records by checking the box next to **Delete**.
6. Within the Mail Servers table, supply the MX record information following the information from the Trend Micro Email Security welcome e-mail.

Enom

1. Login to your account at www.enom.com.
2. From the **Domains** drop-down menu, select **My Domains**. You will see a list of domains associated with your account.
3. Click the domain name that you would like to use.
4. From the **Domain Control Panel**, select **Email Settings** from the **Manage Domain** drop-down list on the right side of the screen. This opens the Edit Email Settings page.
5. In the **Service Selection** drop-down list near the top of the page, select **User (MX)**.
6. Click the **New Row** button to add rows.
7. For each MX Record, supply the MX record information following the information from the Trend Micro Email Security welcome e-mail.
8. Click the **Save** button in the lower-right corner of the screen.

DreamHost

1. Login to your account at www.dreamhost.com.
2. Click **Mail** on the left side and select **MX** from the drop-down menu.
3. Click **Edit** next to the domain you will be using.

4. Under **Custom MX Records**, delete the existing MX record then supply the MX record information following the information from the Trend Micro Email Security welcome e-mail.
5. Click **Update** your custom MX records now.

Yahoo! Small Business

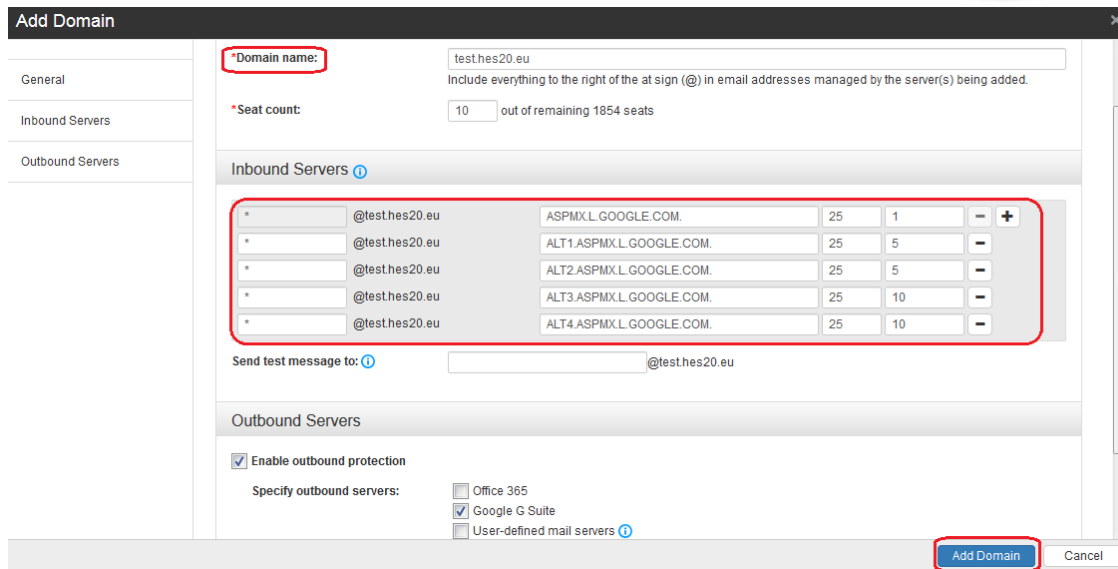
1. Login to your account at smallbusiness.yahoo.com.
2. Click **Domain Control Panel** below the domain you'd like to use with the message security service.
3. Click **Manage Advanced DNS Settings**.
4. Click **Change MX Records**.
5. Clear all existing MX records.
6. Supply the MX record information following the information from the Trend Micro Email Security welcome e-mail.
7. Click **Submit**.

Configuring Trend Micro Email Security to Forward Inbound E-mails to Google Apps Mail Servers

Once Trend Micro Email Security has been setup, you must activate the domains to be used.

After that, Trend Micro Email Security should be configured to forward e-mails to the Google Apps Mail Servers:

1. Login to the Trend Micro Email Security console.
2. Click on **Domains > Add**.
3. Enter the domain name and seats assigned for the domain to be routed.
4. In the **Inbound Servers** field, enter the FQDN of the Google Mail Servers provided to you by Google. In the Google Apps Admin console, this is listed under **Apps > G Suite > Gmail > Advanced Settings > General Settings > MX Records**.



Add Domain

*Domain name: test.hes20.eu
Include everything to the right of the at sign (@) in email addresses managed by the server(s) being added.

*Seat count: 10 out of remaining 1854 seats

Inbound Servers

| | | | | | | |
|---|----------------|-------------------------|----|----|---|---|
| * | @test.hes20.eu | ASPMXL.GOOGLE.COM. | 25 | 1 | - | + |
| * | @test.hes20.eu | ALT1.ASPMXL.GOOGLE.COM. | 25 | 5 | - | |
| * | @test.hes20.eu | ALT2.ASPMXL.GOOGLE.COM. | 25 | 5 | - | |
| * | @test.hes20.eu | ALT3.ASPMXL.GOOGLE.COM. | 25 | 10 | - | |
| * | @test.hes20.eu | ALT4.ASPMXL.GOOGLE.COM. | 25 | 10 | - | |

Send test message to: @test.hes20.eu

Outbound Servers

☒ Enable outbound protection

Specify outbound servers:

☐ Office 365
☒ Google G Suite
☐ User-defined mail servers

Add Domain Cancel

There are several MX records for load balancing. Click the + icon to add additional MX records.

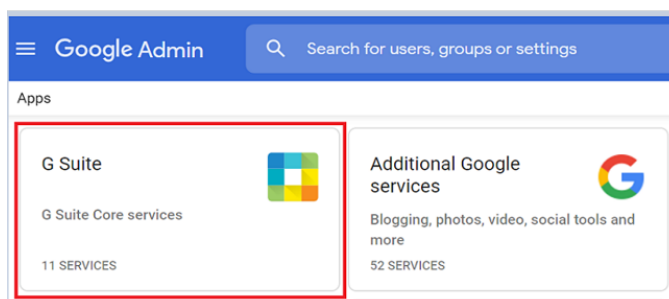
5. Click **Save**.

Configuring Google Apps Mail Servers to Accept Inbound E-mails from Trend Micro Email Security

Google Apps Mail Servers will only accept connections from authorized mail servers.

Below are the steps on how to configure Google Apps Mail Servers to accept incoming e-mail connections from Trend Micro Email Security Servers.

1. Login to the Google Apps Admin Console.
2. Go to **Apps > G Suite > Gmail > Advanced settings**.



Apps > G Suite

Services



Calendar

Organize your schedule and share events with friends.



Drive and Docs

With Google Drive, you can create, share and keep all your stuff in one place. Share files with others, and edit them together in real time.



Gmail

Get a fresh start with email that has less spam



Google Hangouts

HD video, voice or text conversations across all your devices



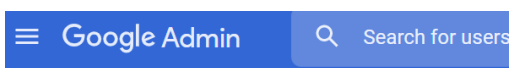
Google+

Google+ at Work



Groups for Business

Create mailing lists and discussion groups



Apps > G Suite > Settings for Gmail

Safety

Configure email and spam safety features

Setup

Configure setup features

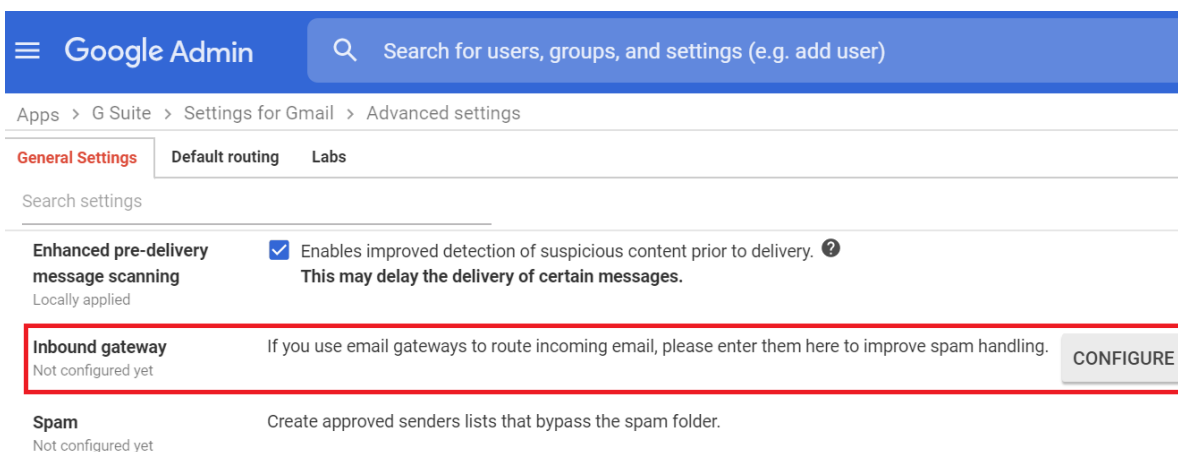
End User Access

Configure end user access features

Advanced settings »

Access other settings for controlling mail flow for the domain.

3. Scroll down to the Inbound gateway settings then click **Configure**.



4. Add the IP addresses of Trend Micro Email Security in the inbound gateway based on your region.

North America, Latin America and Asia Pacific:

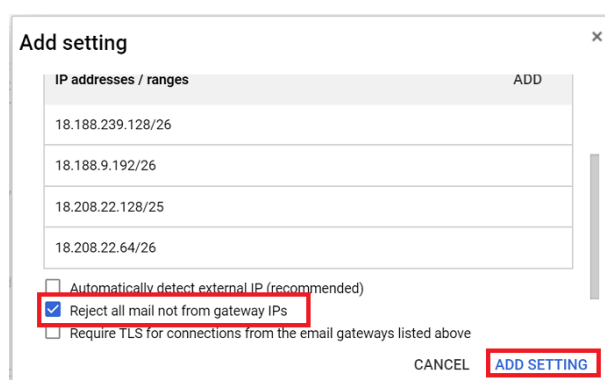
- 18.208.22.64/26
- 18.208.22.128/25
- 18.188.9.192/26
- 18.188.239.128/26

Europe, the Middle East and Africa:

- 18.185.115.0/25
- 18.185.115.128/26
- 34.253.238.128/26
- 34.253.238.192/26

Australia and New Zealand:

- 13.238.202.0 /25
- 13.238.202.128 /26



Note: Checking the “Reject all mail not from gateway IPs” box will ensure that all incoming e-mails will be scanned by Trend Micro Email Security before it is forwarded to Google Apps.

Testing the Message Route

Below are the steps on how to test the message route:

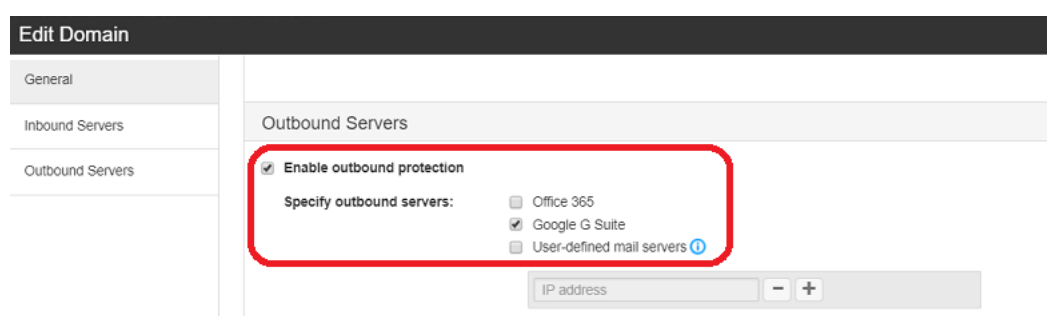
1. Send e-mails from another e-mail service provider (for example, Yahoo or Gmail) to a recipient in your domain. If you receive the e-mail from the other e-mail service provider, the DNS MX record is configured correctly.

2. Search the e-mail in the Mail Tracking logs of Trend Micro Email Security:
 - a. Login to the Trend Micro Email Security administrator console.
 - b. Click on **Logs > Mail Tracking**.
 - c. In the **Direction** dropdown list, select **Incoming**.
 - d. Enter the e-mail details used in the test e-mail.
 - e. If the message passed through, the details will be displayed in the Mail Tracking logs. It will also indicate where the e-mail was delivered.

Scanning Outbound E-mail from Google Apps Mail Servers

Configure your Trend Micro Email Security Settings

1. Login to the Trend Micro Email Security administrator console.
2. Click **Domains**. Choose the domain that you want to configure.
3. **Enable outbound protection** by checking the box next to it.
4. Check **Google G Suite**.
5. Click **Save**.



Edit Domain

General

Inbound Servers

Outbound Servers

Outbound Servers

☒ **Enable outbound protection**

Specify outbound servers:

☐ Office 365

☒ Google G Suite

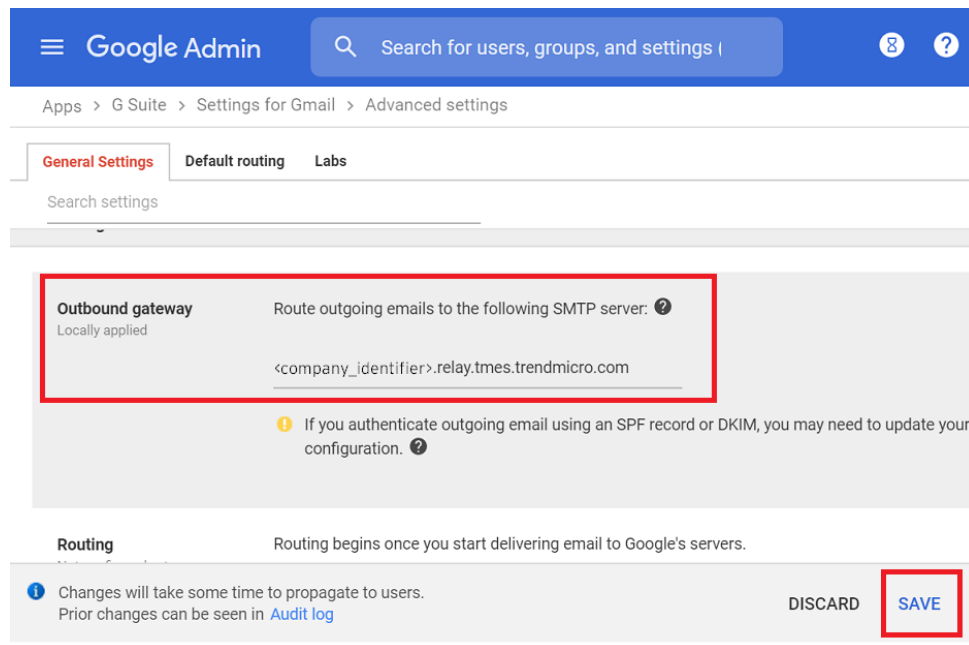
☐ User-defined mail servers ⓘ

IP address - +

Configure Google Apps Settings

1. Login to your Google Apps administrator center account.
2. Go to **Apps > G Suite > Gmail > Advanced settings > General Setting > Outbound gateway**.
3. In Outbound gateway field, add the Fully Qualified Domain Name (FQDN) for the purpose of relaying e-mails to the Trend Micro Email Security MTA Servers based on your region:

- North America, Latin America and Asia Pacific:
<company_identifier>.relay.tmes.trendmicro.com
- Europe, the Middle East and Africa:
<company_identifier>.relay.tmes.trendmicro.eu
- Australia and New Zealand:
<company_identifier>.relay.tmes-anz.trendmicro.com



The screenshot shows the Google Admin console interface. At the top, there's a blue header with the Google Admin logo and a search bar. Below the header, the breadcrumb trail reads: Apps > G Suite > Settings for Gmail > Advanced settings. The 'General Settings' tab is selected, with sub-tabs for 'Default routing' and 'Labs'. A search bar for settings is present. The 'Outbound gateway' section is highlighted with a red box. It shows the text 'Route outgoing emails to the following SMTP server: ?' and a text input field containing '<company_identifier>.relay.tmes.trendmicro.com'. Below this, a yellow warning icon states: 'If you authenticate outgoing email using an SPF record or DKIM, you may need to update your configuration. ?'. The 'Routing' section is partially visible below. At the bottom, a message states: 'Changes will take some time to propagate to users. Prior changes can be seen in Audit log'. To the right of this message are 'DISCARD' and 'SAVE' buttons, with the 'SAVE' button highlighted by a red box.

4. Click **Save**.